

CLAIMS

What is claimed is:

1. A method for configuring encryption strengths for data, comprising the steps of:

- (a) providing a piece of the data with a sensitivity level;
- (b) authenticating a remote user with a clearance level for accessing the data;
- (c) selecting an encryption strength for the piece of the data based on the clearance level of the remote user, if the clearance level of the remote user allows access to the piece of the data with the sensitivity level;

- (d) encrypting the piece of the data; and
- (e) providing access to the encrypted piece of the data to the remote user.

2. The method of claim 1, wherein the providing step (a) comprises:

- (a1) providing the data, wherein each piece of the data has one of a plurality of sensitivity levels.

3. The method of claim 1, wherein the authenticating step (b) comprises:

- (b1) receiving identification data for the remote user;
- (b2) authenticating the identification data of the remote user; and
- (b3) verifying that the remote user has been assigned the clearance level for accessing the data.

4. The method of claim 1, wherein the selecting step (c) comprises:

(c1) receiving a request from the remote user for access to the piece of data;

(c2) determining if the clearance level of the remote user allows access to the

5 piece of data with the sensitivity level; and

(c3) selecting an encryption strength for the piece of data based on the clearance level of the remote user, if the clearance level of the remote user allows access to the piece of data with the sensitivity level.

10 5. The method of claim 1, wherein the authenticating step (b) comprises:

(b1) receiving identification data for the remote user and a request for a session sensitivity level;

(b2) authenticating the identification data;

(b3) verifying that the remote user has been assigned the clearance level for
15 accessing the data; and

(b4) validating the session sensitivity level.

6. The method of claim 5, wherein the validating step (b4) comprises:

(b4i) determining if the session sensitivity level allows the remote user to access
20 pieces of data with sensitivity levels at or below the clearance level for the remote user.

7. The method of claim 1, wherein the selecting step (c) comprises:

(c1) determining pieces of data with sensitivity levels at or below the session sensitivity level to which the clearance level allows the remote user to access; and

(c2) selecting an encryption strength for the pieces of data based on the session sensitivity level.

5

8. The method of claim 1, wherein the selecting of the encryption strength for the piece of the data is also based on the sensitivity level of the piece of the data.

9. The method of claim 1, wherein the selecting of the encryption strength for the piece of the data is also based on a security rating of an output line onto which the encrypted piece of the data will be provided to the remote user.

10. The method of claim 1, further comprising:
(f) blocking access to pieces of data to which the clearance level does not allow the remote user to access.

11. A method for configuring encryption strengths for data, comprising the steps of:

- (a) providing a piece of the data with a sensitivity level;
- (b) authenticating a remote user with a clearance level for accessing the data;
- (c) receiving a request from the remote user for access to the piece of data;
- (d) determining if the clearance level of the remote user allows access to the

piece of data with the sensitivity level;

(e) selecting an encryption strength for the piece of data based on the clearance level of the remote user, if the clearance level of the remote user allows access to the piece of data with the sensitivity level;

5 (f) encrypting the piece of the data; and

(g) providing access to the encrypted piece of the data to the remote user.

12. The method of claim 11, wherein the selecting of the encryption strength for the piece of the data is also based on the sensitivity level of the piece of the data.

10 13. The method of claim 11, wherein the selecting of the encryption strength for the piece of the data is also based on a security rating of an output line onto which the encrypted piece of the data will be provided to the remote user.

15 14. The method of claim 11, wherein the selecting of the encryption strength for the piece of the data is also based on a session sensitivity level.

15. A method for configuring encryption strengths for data, comprising the steps of:

20 (a) providing the data, wherein each piece of the data has one of a plurality of sensitivity levels;

(b) receiving a clearance level assigned to a remote user for accessing the data

and a request for a session sensitivity level;

(c) authenticating the remote user and validating the session sensitivity level;

(d) determining pieces of the data with sensitivity levels at or below the session sensitivity level to which the clearance level allows the remote user to access; and

5 (e) selecting an encryption strength for the pieces of the data based on the session sensitivity level;

(f) encrypting the pieces of the data; and

(g) providing access to the encrypted pieces of the data to the remote user.

10 16. The method of claim 15, wherein the authenticating step (c) comprises:

(c1) determining if the session sensitivity level for the remote user allows the remote user to access pieces of data with sensitivity levels at or below the clearance level for the remote user.

15 17. The method of claim 15, wherein the selecting of the encryption strength for the pieces of the data is also based on the clearance level of the remote user.

18. The method of claim 15, wherein the selecting of the encryption strength for the pieces of the data is also based on the sensitivity level of each piece of the data.

20 19. The method of claim 15, wherein the selecting of the encryption strength for the pieces of the data is also based on a security rating of an output line onto which the

encrypted pieces of the data will be provided to the remote user.

20. A computer readable medium with program instructions for configuring encryption strengths for data, comprising the instructions for:

- (a) providing a piece of the data with a sensitivity level;
- (b) authenticating a remote user with a clearance level for accessing the data;
- (c) selecting an encryption strength for the piece of the data based on the clearance level of the remote user, if the clearance level of the remote user allows access to the piece of the data with the sensitivity level;
- (d) encrypting the piece of the data; and
- (e) providing access to the encrypted piece of the data to the remote user.

21. The medium of claim 20, wherein the providing instruction (a) comprises instructions for:

- (a1) providing the data, wherein each piece of the data has one of a plurality of sensitivity levels.

22. The medium of claim 20, wherein the authenticating instruction (b) comprises instructions for:

- (b1) receiving identification data for the remote user;
- (b2) authenticating the identification data of the remote user; and
- (b3) verifying that the remote user has been assigned the clearance level for

accessing the data.

23. The medium of claim 20, wherein the selecting instruction (c) comprises instructions for:

- (c1) receiving a request from the remote user for access to the piece of data;
- (c2) determining if the clearance level of the remote user allows access to the piece of data with the sensitivity level; and
- (c3) selecting an encryption strength for the piece of data based on the clearance level of the remote user, if the clearance level of the remote user allows access to the piece of data with the sensitivity level.

24. The medium of claim 20, wherein the authenticating instruction (b) comprises instructions for:

- (b1) receiving identification data for the remote user and a request for a session sensitivity level;
- (b2) authenticating the identification data and validating the session sensitivity level;
- (b3) verifying that the remote user has been assigned the clearance level for accessing the data; and
- (b4) validating the session sensitivity level.

25. The medium of claim 24, wherein the validating instruction (b2) comprises

instructions for:

(b4i) determining if the session sensitivity level allows the remote user to access pieces of data with sensitivity levels at or below the clearance level for the remote user.

5 26. The medium of claim 20, wherein the selecting instruction (c) comprises instructions for:

(c1) determining pieces of data with sensitivity levels at or below the session sensitivity level to which the clearance level allows the remote user to access; and

(c2) selecting an encryption strength for the pieces of data based on the session sensitivity level.

10 27. The medium of claim 20, wherein the selecting of the encryption strength for the piece of the data is also based on the sensitivity level of the piece of the data.

15 28. The medium of claim 20, wherein the selecting of the encryption strength for the piece of the data is also based on a security rating of an output line onto which the encrypted piece of the data will be provided to the remote user.

29. The medium of claim 20, further comprising instructions for:

20 (f) blocking access to pieces of data to which the clearance level does not allow the remote user to access.

30. A computer readable medium with program instructions for configuring encryption strengths for data, comprising the instructions for:

- (a) providing a piece of the data with a sensitivity level;
- (b) authenticating a remote user with a clearance level for accessing the data;
- (c) receiving a request from the remote user for access to the piece of data;
- (d) determining if the clearance level of the remote user allows access to the piece of data with the sensitivity level;
- (e) selecting an encryption strength for the piece of data based on the clearance level of the remote user, if the clearance level of the remote user allows access to the piece of data with the sensitivity level;
- (f) encrypting the piece of the data; and
- (g) providing access to the encrypted piece of the data to the remote user.

31. The medium of claim 30, wherein the selecting of the encryption strength for the piece of the data is also based on the sensitivity level of the piece of the data.

32. The medium of claim 30, wherein the selecting of the encryption strength for the piece of the data is also based on a security rating of an output line onto which the encrypted piece of the data will be provided to the remote user.

33. The medium of claim 30, wherein the selecting of the encryption strength for the piece of the data is also based on a session sensitivity level.

34. A computer readable medium with program instructions for configuring encryption strengths for data, comprising the instructions for:

- (a) providing the data, wherein each piece of the data has one of a plurality of sensitivity levels;
- (b) receiving a clearance level assigned to a remote user for accessing the data and a request for a session sensitivity level;
- (c) authenticating the remote user and validating the session sensitivity level;
- (d) determining pieces of the data with sensitivity levels at or below the session sensitivity level to which the clearance level allows the remote user to access; and
- (e) selecting an encryption strength for the pieces of the data based on the session sensitivity level;
- (f) encrypting the pieces of the data; and
- (g) providing access to the encrypted pieces of the data to the remote user.

35. The medium of claim 34, wherein the authenticating instruction (c) comprises instructions for:

- (c1) determining if the session sensitivity level allows the remote user to access pieces of data with sensitivity levels at or below the clearance level for the remote user.

36. The medium of claim 34, wherein the selecting of the encryption strength for the pieces of the data is also based on the clearance level of the remote user.

37. The medium of claim 34, wherein the selecting of the encryption strength for the pieces of the data is also based on the sensitivity level of each piece of the data.

5 38. The medium of claim 34, wherein the selecting of the encryption strength for the pieces of the data is also based on a security rating of an output line onto which the encrypted pieces of the data will be provided to the remote user.

TOP SECRET